**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF TEXAS**
**SAN ANTONIO DIVISION**

**MELODY JOY CANTU and**
**DR. RODRIGO CANTU,**

***Plaintiffs,***

**v.** **Case No. SA-20-CV-0746-JKP**

**DR. SANDRA GUERRA and**
**DIGITAL FORENSICS**
**CORPORATION,**

***Defendants*.**

**MEMORANDUM OPINION AND ORDER**

Before the Court are five related motions: (1) a *Motion for Summary Judgment* (ECF No. 109) filed by Defendant/Counter-plaintiff Dr. Sandra Guerra ("Guerra"); (2) a *Motion for Summary Judgment* (ECF No. 110) filed by Plaintiffs/Counter-defendants Melody Joy Cantu ("MC") and Dr. Rodrigo Cantu (collectively "the Cantus"); (3) a *Motion for Leave to File Sur-Reply* (ECF No. 119) filed by Guerra; (4) *Plaintiffs' Motion for Leave to File Supplemental Motion for Summary Judgment* (ECF No. 120); and (5) a *Motion for Leave to File Defendants' Sur-Reply* (ECF No. 124) filed by Defendants with respect to the motion for leave to file supplemental motion. The Court finds no reason to await a response on the last motion. With relevant briefing by Plaintiffs (ECF Nos. 112 and 118), Guerra (ECF Nos. 114 and 121), and Defendant Digital Forensics Corporation ("DFC") (ECF No. 115 (motion for leave); Ex. B ("DFC Response" attached to motion for leave); ECF No. 121), [1] the four initial motions are fully briefed or the time for further briefing has passed. After considering the motions, related briefing, relevant pleadings, submitted

[1] DFC filed its response with leave of Court. *See* Text Order of Nov. 1, 2022 (granting leave and directing the Clerk of Court to file Exhibit B as DFC's response). DFC's response expressly joins and incorporates Guerra's response. *See* DFC Resp. For unknown reasons, the Clerk of Court never filed Exhibit B as a separate response. Nevertheless, the Court will consider the exhibit as DFC's response.

evidence,[2] and applicable law, the Court partially grants the motion for summary judgment filed by Guerra and denies the other motions.

## I. PROCEDURAL BACKGROUND

At its core, this action relates to relationship disputes involving the Cantus and Guerra. The Cantus commenced this case on June 24, 2020, by filing a civil complaint alleging various claims against Guerra and DFC, a forensics company she retained. *See* ECF No. 1. Within a month, Plaintiffs had filed two amended complaints (ECF No. 3 and 6), the latter merely correcting the first. As characterized by the Cantus:

> This is an action for violations of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et. seq. ("CFAA"), the Federal Wiretap Act, 18 U.S.C. §§ 2510 et. seq., the Texas Harmful Access by Computer Act ("HACA"), Texas Penal Code § 33.02(b-1)(1), and the Texas torts of malicious prosecution and intentional infliction of emotional distress.

First Am. Compl. ("FAC") (ECF No. 6) ¶ 1. They assert fourteen claims. *See id*. ¶¶ 54-124. Claims 1 through 8 arise under the CFAA, *see id*. ¶¶ 54-92; Claims 9, 10, and 11 arise under the HACA and the Texas Penal Code, *see id*. ¶¶ 93-108; Claim 12 arises under the Federal Wiretap Act, *see*

[2] Both sides have submitted numerous exhibits with their various filings. Guerra provides twelve exhibits with her motion for summary judgment, *see* ECF No. 109-1 through 109-12 (Exs. 1 through 12); ten exhibits with her response, *see* ECF No. 114-1 through 114-10 (Exs. A through J); and fifteen exhibits with her proposed surreply, *see* ECF No. 119-3 to 119-17 (Exs. K through Y). Plaintiffs submit nineteen exhibits with their motion, *see* ECF No. 110-1 to 110-19 (Exs. A through S, including a proposed order (Ex. S); twenty exhibits with their response, *see* ECF No. 112-1 to 112-20 (the same Exs. A through R, with a new Ex. S and Ex. T); and twenty-three exhibits with their reply, *see* ECF No. 118 1 to 118-23 (the same Exs. A through T as ECF No. 112, with new Exs. U, V, and X (there is no Ex. W, even though Ex. W is referenced in footnote 6 of the reply)). For ease of reference, the Court will cite to Guerra's exhibits by ECF No. and to Plaintiffs' exhibits by the reference letter used in their reply.

Plaintiffs have indicated that they have withheld four exhibits (Exs. D, I, N, and O) but will provide such exhibits for *in camera* review in accordance with the protective order (ECF No. 88) entered in this case. Paragraph 13 of that order addresses the manner of use in proceedings and permits parties to provide confidential information "solely for *in camera* review" when "appropriate (e.g., in connection with discovery and evidentiary motions)." While the Court sees the argument for viewing a summary judgment motion as an evidentiary motion, such designation seems more appropriate for motions in limine addressing the admissibility of evidence. The typical means to use confidential information within the context of summary judgment is to redact unnecessary portions and/or move to seal the information consistent with the sealing requirements of the Court. Paragraph 13 provides for filing under seal as an option to present confidential information to the Court. Of course, being subject to a confidentiality protective order does not of itself qualify a submission as worthy of being sealed. Given Plaintiffs' interpretation of paragraph 13 of the protective order, the Court requested the withheld exhibits by emails dated July 20 and July 24, 2023. Although an attorney for Plaintiffs indicated via email response that he will take care of this matter, no one has submitted the withheld exhibits to the Court's knowledge. The Court thus proceeds without the withheld exhibits.

*id*. ¶¶ 109-11; and Claims 13 (malicious prosecution) and 14 (intentional infliction of emotional distress) arise under Texas law, *see id*. ¶¶ 112-14.

Guerra thereafter filed an amended answer and counterclaims (ECF No. 37) with court approval. With respect to her counterclaims, she states:

> This is an action for violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(c); the Harmful Access by Computer Act, Tex. Pen. Code § 33.02(a); and the Texas torts of stalking, defamation, intentional infliction of emotional distress, and abuse of process.

Am. Answer ¶ 1.[3] Defendant DFC filed its answer simultaneously with a motion to dismiss that the Court later denied. *See* ECF No. 16 (motion to dismiss and answer); ECF No. 51 (order denying motion to dismiss).

These filings provide the live pleadings of the parties. Because the Court dismissed Guerra's abuse-of-process counterclaim, *see* ECF No. 53 at 36, that counterclaim is no longer at issue.

Guerra seeks summary judgment on Plaintiffs' computer and wiretap claims on grounds that Plaintiffs lack evidence that (i) either defendant intentionally or knowingly hacked or surveilled Plaintiffs or (ii) Plaintiffs suffered the requisite damages for such claims. ECF No. 109 at 2. Additionally, she invokes collateral estoppel as a bar to all claims asserted by Dr. Cantu. *See id*. at 2, 4. Plaintiffs seek summary judgment against both defendants on their Claims 1-11 and 13. *See* ECF No. 110 at 4.[4] Neither side seeks summary judgment on any counterclaim.

When the parties filed their motions for summary judgment, they were simultaneously engaging in several discovery disputes that were set for hearing for November 4, 2022. *See* ECF No. 108 (setting in-person hearing on three discovery motions); ECF No. 113 (adding another motion

[3] The counterclaims commence on page thirteen and restarts paragraph numbering at one. References to paragraph numbers are to her counterclaims.

[4] Because Plaintiffs' motion lacks page numbers, the Court utilizes the page numbers provided by its electronic filing system.

to compel to the hearing). The Magistrate Judge, however, cancelled the hearing because the parties advised that they had agreed "that there are no matters currently set for hearing . . . which require resolution by the Court." *See* ECF No. 117. The Court thus devotes no time to the various allegations of withheld documents relative to the instant motions. *See, e.g.*, ECF No. 109 at 4 ("reserv[ing] the right to amend and/or supplement this Motion pending the Court's ruling on [discovery] motions and the production of any documents that may be ordered by the Court"); ECF No. 110 at 7-10 (discussing sanctions for discovery abuses, asserting a willful failure of DFC to produce documents, and discussing evasive discovery responses); ECF No. 112 at 6-7 (setting out legal principles related to sanctions for spoliation of evidence), 9-10 (contending that both defendants "have willfully withheld discovery related to the computer intrusions, as was revealed in depositions and by their belated piecemeal productions which indicate there is missing discovery"). To the extent these issues remain unresolved, the parties should have resolved them before the Magistrate Judge. No party, furthermore, has complied with the requirements of Fed. R. Civ. P. 56(d) as to why they cannot present facts to justify their positions.

## II. FACTUAL BACKGROUND[5]

Neither side provides much of a factual background supported by citations to the record. While pleading allegations do not provide evidentiary support for motions for summary judgment, they can provide helpful detail when uncontested. The Court gleans some uncontested background facts from the pleadings. When Plaintiffs filed their operative complaint in this action, they were a married couple residing in Boerne, Texas, and Guerra resided in San Antonio. *See* FAC ¶¶ 7-8, 15; Am. Answer ¶¶ 7-8, 15.

Prior to the Cantus' marriage, Dr. Guerra and Dr. Cantu had been married for ten years and had two daughters together. *See* FAC ¶¶ 16-17; Am. Answer ¶¶ 16-17. The doctors divorced in

[5] The factual background is uncontested unless otherwise noted.

2009. *See* FAC ¶ 16; Am. Answer ¶ 16. The Cantus married in 2014, but the marriage ended in 2016 even though they continued to secretly keep their relationship going. *See* FAC ¶¶ 18, 20; Am. Answer ¶¶ 18, 20. That secret ended on April 1, 2018, when MC observed Drs. Guerra and Cantu having dinner with their daughters. *See* FAC ¶¶ 22-23; Am. Answer ¶¶ 22-23. At some later point, the Cantus remarried. *See* FAC ¶ 7; Am. Answer ¶ 7.

On or about May 16, 2018, Guerra hired DFC. *See* FAC ¶ 27; Am. Answer ¶ 27. Through an affidavit dated August 18, 2018, she avers that she "retained the services of DFC dba Digital Investigations and . . . authorized them to request information on [her] behalf." *See* Ex. A at 2. She authorized and requested that "every Interest [sic] Service Provider (ISP), phone service provider (PSP), online service provider (OSP) . . . having custody or control of any documents, records, and other information pertaining to [her] to furnish to DFC any such information." *Id*. This authorization would expire on December 31, 2018. *Id*. She paid DFC $3,000 to investigate "who was attempting to hack [her] and sign [her] up on accounts without [her] authorization." *See* Dep. Guerra 6:18-7:4 (Ex. C).

On August 21, 2018, MC "received a text on her smartphone with a hidden tracking link," which she clicked "thinking it was a normal business appraisal request." *See* FAC ¶ 33; Am. Answer ¶ 33. That same link appears in the Phase I Report with instructions to Guerra as to "how to deploy it against the Cantus." *See* FAC ¶ 34; Am. Answer ¶ 34.

Plaintiffs present three August 21, 2018 emails in Ex. E that they contend in a parenthetical that Guerra forwarded to DFC from fake email addresses from which she had phished Plaintiffs by sending URL tracking links: (1) from "Melissa McCarthy" to DFC forwarding an email from McCarthy to Aggiemed98@yahoo.com; (2) from "Teresa Fuentes" to DFC forwarding an email from Fuentes to joyandtyrus@hotmail.com; and (3) from "Thomas Smite" to DFC attaching a screenshot message to "Melody" that contains a tracking URL. *See* ECF No. 112 at 4 n.7 (citing Ex. E with parenthetical); Ex. E at 1-4. Each of these three emails have "157307" in the Subject

line. *See* Ex. E. 1-4.

On August 22, 2018, DFC provided Guerra a "Phase I Evaluation Report" for Case Number 157307. *See* Ex. B (Bates # Guerra 62-87). It shows that Guerra directed DFC to "Conduct a digital investigation on a known suspect" and to "Discover the identity of an unknown cyber-harasser." *Id*. at 64. As background information, it states that Guerra "has been a victim" of "an unknown person" who (1) attempted to hack her phone by attempting to intrude into her mobile phone account; (2) engaged in identity theft and misappropriation by creating accounts on dating websites using Guerra's email address; and (3) defamed her by making untrue statements. *Id*. The background information further states that Guerra "has also been the victim of harassment caused by [MC] when Guerra's social network received unwanted messages disparaging [Guerra's] character." *Id*.

The Report sets out the objectives of Phase I and the parameters for the scope of work. *See id*. at 65. In general, the objective was "to record and document the online harassment, harm, or defamation." *Id*. To achieve this objective, Phase I would include "the collection, extraction, recovery, and preservation of all data from available client devices and online accounts and performing an extensive search of the online presence of the suspects based on the information provided." *Id*. As part of Phase I, "tracking URLs" would be created "to target at the suspect(s)." *Id*. The client – Guerra – would then "send the tracking URLs to the suspect(s) and [DFC would] monitor the tracking URLs for any activity by the suspect(s)." *Id*.

Through its Phase I investigation, DFC acquired evidence documenting (1) attempted hacking of Guerra's Verizon phone by an unknown person on eight dates between May 16 and June 6, 2018; (2) identity theft and misappropriation by an unknown individual; and (3) online harassment by Facebook user "Joy Brown" and LinkedIn user "Melody Joy Cantu," both of which Guerra believed to be Plaintiff MC. *Id*. at 68-73. A web investigation located a Facebook profile for Joy Cantu with a match with Joy Brown. *See id*. at 74-75. A comprehensive report dated August

21, 2018, by DFC shows various names used by Melody Joy Cantu, including Melody Joy Brown and Joy Brown, and three associated emails, including the Hotmail one that received an email from "Teresa Fuentes." *See id*. at 76; Ex. E at 3.

As part of the Phase I investigation, DFC created "Tracking URLs," which are links that send information to the link creator when clicked. Ex. B at 77. When clicked, these URLs capture "IP address, operating system, browser, screen resolution, and hash information for the device" used to click the link. *Id*. These created URLs were for Guerra "to send or target at the suspects." *Id*. In order to avoid false positives, Guerra was asked to use her devices on initial URLs so that DFC could exclude her IP addresses if she were to accidentally click a URL later. *Id*. DFC created two "Client-directed tracking URLs" – one for "Melody_Cantu" and one for "Rodrigo_Cantu" – and three "DFC-directed tracking URLs" labeled as: (1) "Melody_Joy_From_Teresa"; (2) "Dr.Cantu_From_Melissa"; and (3) "Melody_Joy_via_Phone." *Id*. at 80.

The third DFC-directed URL is the same link MC received on August 21, 2018. *Compare* FAC ¶¶ 33-34; Am. Answer ¶¶ 33-34 *with* Ex. B at 80-82. This third link sent IP address information to DFC on August 21, 2018, from a Macintosh ("Mac") operating system and an iPhone. *See* Ex. B at 82. As of the date of the Phase I report, this was the only information transmitted to DFC from any tracking URL created for Guerra. *See id.* at 82-84 (showing no other transmitted information). This tracking URL corresponds to an emailed screen shot. *Compare id*. at 82 *with* Ex. E at 4-5. Further investigation of the transmitted information showed a very similar IP address (72.179.164.76) for the Mac and iPhone as compared to the IP address (72.179.171.30) for the person who had engaged in identity theft and misappropriating by creating fake social media profiles using Guerra's email address. *Compare id*. at 69-70 *with id*. at 82. Both individuals, furthermore, were located at the same latitude, longitude, and postal code. *Compare id*. at 70 *with id*. at 82.

On September 4, 2018, Guerra filed a police report against MC accusing her of harassment and telling the police officer that she (Guerra) had to file the report if she wanted to proceed with Phase II of the investigation being conducted by DFC. *See* FAC ¶ 40; Am. Answer ¶ 40. This requirement is consistent with the Phase I Report. *See* Ex. B at 66.

On November 15, 2018, MC's employer initiated an investigation into the security of her work computer based upon an allegation that, on or about October 10, 2018, Guerra "may have hacked her business computer and breached her VPN firewall and router." ECF No. 109-2 at 74. The employer spoke to a "Spectrum cable representative that was on property at [MC's] residence" and he "advised that the cable splitter that was on [her] personal line appears to have been attached by Spectrum cable but he was not sure why it was done." *Id*. Her "dedicated business line did not appear to have been tampered with or compromised" and the "investigation did not reveal any breach of [the employer's] data." *Id*. MC advised that the San Antonio Police Department "cyber-security unit was going to accept her case of computer hacking regarding her personal account." *Id*.

The next day, the employer's "review of [MC's] equipment and data did not reveal any breach or corruption." *Id*. After concluding that its "investigation did not reveal any breach of [its] data at [MC's] residence," the employer closed the investigation as "Unsubstantiated." *Id*. at 74-75.

On November 20, 2018, a Bexar County Assistant Criminal District Attorney filed a criminal Information against MC based upon a Probable Cause Affidavit of Jo Ann Cano who relied on an offense report of Detective E. Gallardo made from statements of Guerra. *See* Ex. H. The Information charged MC of harassment occurring on or about April 1, 2018, when "with intent to harass, annoy, alarm, torment, and embarrass" Guerra, MC sent "repeated electronic communications" to Guerra "in a manner reasonably likely to harass, annoy, alarm, torment, and embarrass" Guerra. *Id*. The Information alleged the following acts by MC: (1) contacting Guerra's "social

media contacts using a social media platform, (2) accessing Guerra's "wireless account without . . . consent; and (3) contacting Guerra "on social media." *Id*.

Detective Gallardo based the offense report on statements of Guerra. *See id*. Detective Gallardo noted that, not only did Guerra make the allegations stated in the Information, but Guerra was able to positively identify MC because (1) she knew MC; (2) a hired digital forensics firm concluded that the IP address for the account that attempted to access Guerra's wireless account was from the same area in which MC lived; (3) MC had contacted the ex-wife of Guerra's new boyfriend and told him that Guerra "has a sexually transmitted disease and that [the ex-wife] should not trust [Guerra] around [their] kids"; (4) MC used social media to contact the ex-wife; (5) Guerra does not have a sexually transmitted disease; (6) MC contacted Guerra's employer to make a false report in hopes to get Guerra fired; and (7) MC has repeatedly contacted Guerra on social media and mentioned an embarrassing video that MC might release electronically. *Id*.

Based on the affidavit of Cano, a county judge found probable cause. *Id*. Bexar County issued an arrest warrant for MC on November 20, 2018, and she was arrested on December 21, 2018. *Id*.

On January 3, 2019, MC retained Exhibit A Computer Forensic Investigations, LLC ("EACFI") to conduct a digital forensic investigation. *See* Ex. P (Dr.CantuProd#000001 through 000028) at 5. Later that month, EACFI billed MC for a dark web email scan. *See id*. at 6.

Plaintiffs commenced this action in June 2020. And during discovery, on July 18, 2022, Plaintiffs deposed Shawn Kasal, who appeared "in the capacity of a digital forensics expert" for DFC. Dep. Kasal 5:11-14 (Ex. G). He testified about coaxial cables and how one can splice in a signal splitter that can provide a means to surveil or record information traveling over the cable if one had an adequate understanding of various methodologies. *Id*. 6:10-8:3. When asked whether he has "ever spliced into coaxial cable to monitor any signals," he stated that he would be "under a protective order for any such operation." *Id*. 8:10-13. He explained that he "was employed by a

cable Internet provider and under [a non-disclosure agreement] and protective order." *Id*. 8:23-24. He further testified that, other than the circumstances under the protective order, there had been no other time that he "ever spliced into a coaxial cable to monitor signal traffic on that cable." *Id*. 9:18-25.

Kasal also testified about the various stages of the process utilized by DFC, as well as the capabilities of the tracking code DFC created. *Id*. 18:20-37:11. He "reviewed the Phase I report and nothing else in connection with this matter." *Id*. 51:14-16; *accord*, *id*. 26:20-21,41:19-21. He based his testimony on what he read in the Phase I Report. *Id*. 42:3-5. When questioned about code "existing on the computer," he answered that he did not understand how "the actual code . . . existing on the computer . . . would be any different tha[n] what's in the Phase I report." *Id*. 42:7-10. When questioned about whether the code he reviewed was "everything in the package," he stated that he did not understand why DFC would redact anything from his review. *Id*. 42:13-20. Indeed, he testified that general counsel responded with "no" when he asked whether there was "any additional information as it pertains to th[e] code that [he was] not aware of" or whether there was "any hidden features and functions that are not enumerated or described in [the Phase I] report." *Id*. 42:24-43:8.

It was Kasal's understanding that DFC did not implement the IP tracking, but it provided the client with the utility to use IP tracking. *Id*. at 18:21-25. He described "a package" that DFC produced as a way "to try to gain the identity or geolocation information of someone online," which DFC then sent to the client "who was responsible for its implementation and use." *Id*. 19:9-14. His understanding was the end-user would send a code that, when clicked, would reveal "the IP address and possible geolocation information of that . . . visit." *Id*. 19:17-22. This was not "GPS tracking"; the link would instead "get the geolocation of whatever device possibly had clicked on the link whether it be a phone or a laptop or a tablet." *Id*. 19:23-20:8. In other words, the link would provide a snapshot of certain information as of the time it was clicked.

The package included "multiple stages and that tracking link was just one component of the stages within that package." *Id*. 20:22-24. Kasal testified:

> Stage 1 is the ways and means and the snippet of code that could be implemented to determine – to send whether it be a link on social media, e-mail or text message that the end[-]user would click on that would produce some returning information being the IP address, possible geolocation and some basic system information, like, maybe the browser version or the UUID of the session that the user was in. It did not install any piece of malware or any kind of persistent threat to the device.

*Id*. 21:7-15. He testified that he reached the above conclusion from reviewing the code embedded in the link that DFC provided. *Id*. 21:17-22:3. Stage 2 of the package involved "getting legal counsel to assist [the end-user] in the use of [the package]." *Id*. 23:2-5.

When the questioning attorney sought to have Kasal testify that he "reviewed the code that comprised this phishing link" in this case, Kasal avoided the "phishing link" characterization and stated: "I saw what lines of information were embedded in the link that was possibly used for the identification." *Id*. 24:4-8. He testified that he saw those lines in "Raw text." *Id*. 24:9-10. He later explained that he saw the raw text files when he looked at the "code that was contained in the tracking link." *Id*. 27:12-15. He did not review logs of any type or any forensic images of any device. *Id*. 27:16-20.

Kasal recognized that there are various ways to track people "on the Internet or their iPhones." *Id*. 28:21-29:20. And while he agreed that technology exists to "target specific phones and gather a host of information from the phone," that technology was not used with the code he reviewed. *Id*. 29:9-20. He testified that he knows "what malware is" and defined it as "computer code written with a nefarious intent or purpose." *Id*. 29:21-25. He agreed that a nefarious intent or purpose includes "tak[ing] control of someone's phone without their consent" and "monitor[ing] someone's conversations without their consent" through their phone, and that one could use a link to install malware on a phone. *Id*. 30:1-22. But he also testified that those examples were "apart and separate from this instance of that type of technology." *Id*. 30:8-9.

Similarly, while there are "a number of commercially available programs that one can purchase to install malware on someone's iPhone," such "code was not used here." *Id*. 31:13-19. His examination of the code within the tracking links, provided him "some degree of certainty [to] say that it was not an advanced persistent threat and it did not have the capabilities of that type of attack service." *Id*. 31:22-32:1. He reviewed "the embedded code in that tracking link that was offered as part of the solutions package in this matter" and it contained no "capabilities of persistence or infiltration past the identification of very simpl[e] information that one could get or any web provider could get as embedded in website that is worth further specificity here." *Id*. 32:15-20. But he did not see "how the package was deployed." *Id*. 32:23-25. Although he "did not see any result of the implementation of this code," he did not "know how it would be dissimilar from the payload as it is as [he] had a chance to review." *Id*. 33:6-8. He was "unaware of [DFC] adding or subtracting anything to the package past what [he] had opportunity to review." *Id*. 33:8-10.

While Kasal also agreed that it is "possible to anonymously collect and analyze traffic on the Internet for an individual or even a group anonymously," he did so with a "very specific and nuanced answer," which basically limited the capability to the network carrier or internet service provider absent "a warrant or subpoena from the government." *Id*. 34:8-21. He testified that "[t]here are multiple types of phishing" – it "can be used as a social engineering method to glean intelligence for information," it can be "a larger part of a fraud or misuse," it "can be a means of identification," and it has multiple other definitions. *Id*. 35:16-22. Sending a link with a deceptive message to click on a tracking link is a form of social engineering that "could be construed" as deceptive. *Id*. 37:1-7. But he disagreed that "social engineering is a type of fraud"; instead, it "is a form of negotiation." *Id*. 37:8-11.

With discovery disputes ongoing, *see* ECF No. 108 (setting in-person hearing for November 4, 2022, on various discovery motions), the parties filed their motions for summary judgment on October 14, 2022. A month later, Guerra moved to file a surreply. Last month, Plaintiffs filed

their motion for leave to file supplemental motion for summary judgment. And Defendants have recently filed another motion for leave to file a surreply. The Court will first address these latter motions.

## III. LEAVE TO FILE SURREPLY

Defendant Guerra seeks leave to file a surreply to address arguments and evidence first presented by Plaintiffs in their reply to their motion for summary judgment. *See* ECF No. 119 at 1-4. In addition, Defendants jointly seek leave to file a surreply related to Plaintiffs' motion for leave to file a supplemental motion for summary judgment. *See* ECF No. 124.

"As a general practice, neither the Federal Rules of Civil Procedure nor the local rules of this Court permit the filing of a surreply." *Silo Rest. Inc. v. Allied Prop. & Cas. Ins. Co.*, 420 F. Supp. 3d 562, 570 (W.D. Tex. 2019). The local rules, however, leave open the possibility for a party to seek leave to file a post-reply submission. *See* W.D. Tex. Civ. R. 7(e)(1) (formerly 7(f)(1)).

Even though "surreplies are heavily disfavored," it is ultimately "within the sound discretion of the courts to grant or deny leave to file such additional briefing." *Mission Toxicology, LLC v. Unitedhealthcare Ins. Co.*, 499 F. Supp. 3d 350, 359 (W.D. Tex. 2020) (citations and internal quotation marks omitted). However, the circumstances here simply provide no reason for the Court to exercise its discretion to permit either proposed surreply. It is unnecessary to consider either surreply given the Court's rulings on the motions for summary judgment and motion for leave to file a supplemental motion for summary judgment, as set forth more fully below. Defendants seek to file the additional briefs to address arguments and evidence that do not alter the ultimate rulings of the Court. Accordingly, the Court finds no need for additional briefing and denies both motions for leave to file a surreply.

## IV. LEAVE TO FILE SUPPLEMENTAL MOTION

Pursuant to Fed. R. Civ. P. 56(c), Plaintiffs seek leave to file a supplemental motion for summary judgment. They submit that DFC provided supplemental discovery on November 11,

2022, which includes evidence pertinent to this case. Because Plaintiffs still viewed the discovery production to be deficient, they requested further production via letter dated December 12, 2022. They contend that DFC has still not yet produced the withheld discovery. To support their motion for leave, Plaintiffs provide seven exhibits (Exs. A through G). Although they contend that they have filed Exhibit A "under seal" and have emailed the exhibit to opposing counsel and the Court, they actually emailed it to the Court for *in camera* review. Making a filing under seal is not the same as submitting it for *in camera* review.

In their joint response, Defendants point out that discovery expired on September 15, 2022; dispositive motions were due on October 14, 2022; and that Plaintiffs never moved to extend the dispositive motion deadline even though the Magistrate Judge had set a hearing for November 4, 2022, to address unresolved discovery motions. They further point out that Plaintiffs did not file the motion for leave to file a supplemental motion until nine months after the dispositive motion deadline and eight months after produced discovery on November 11, 2022, which Plaintiffs seek to use to supplement the summary judgment record. Defendants further submit that, through the motion for leave to file supplemental motion, Plaintiffs also seek to add new arguments regarding their malicious prosecution claims and utilize summary judgment evidence that was available to Plaintiffs and was produced by Plaintiffs moths before the dispositive motions were due.

Defendants urge the Court to deny the requested supplementation because Plaintiffs have not shown good cause for filing their untimely supplemental motion for summary judgment. They also seek sanctions against Plaintiffs and/or their counsel under Fed. R. Civ. P. 11(c)(2) and/or 16(f)(1)(C) for Plaintiffs filing a frivolous motion and for their absolute failure to disclose that they were also seeking leave to supplement the summary judgment record with evidence and arguments that were readily available to Plaintiffs when they filed their original motion for summary judgment and summary judgment briefing.

For the reasons stated by Defendants, *see* ECF No. 121 at 3-6, the Court denies the motion

to supplement for Plaintiffs' failure to show good cause to file a supplemental motion for summary judgment record substantially past the dispositive motion deadline. The Court adds an additional point. Plaintiffs purport to move to supplement based on Fed. R. Civ. P. 56(c), but the Court sees no relevancy of that provision to requesting supplementation.[6]

Although the Court agrees that Plaintiffs have not shown good cause for their motion for leave to file a supplemental motion, it disagrees that sanctions are warranted. As to requested sanctions under Rule 11, Defendants have failed to comply with the safe-harbor provision within Rule 11(c)(2). By raising the request for sanctions in their response to the motion to supplement, Defendants have not made their "motion for sanctions . . . separately from any other motion," as required by the rule. Defendants, moreover, have not accorded Plaintiffs an opportunity to withdraw or appropriately correct the motion as contemplated by Rule 11(c)(2).

As to requested sanctions under Rule 16(f)(1)(C), the Court finds no sanctionable conduct based on the filing of the motion for leave. Rule 16(f)(1)(C) provides discretion to the federal courts to "issue any just orders" when a litigant or its attorney "fails to obey a scheduling order or other pretrial order." To be sure, Plaintiffs filed their motion for leave to file a supplemental motion for summary judgment well after the deadline for dispositive motions imposed by the Court's scheduling order. But when a deadline has passed, neither litigants nor their attorneys fail to obey the scheduling order merely because they move to supplement past the deadline. Indeed, in such circumstances, the movant recognizes the authority of the scheduling order and seeks leave of Court to act despite the elapsed deadline. The same is true when a party seeks to extend a scheduling order deadline after its expiration. Defendants have pointed to nothing to show that Plaintiffs

[6] Perhaps Plaintiffs intended to rely upon Fed. R. Civ. P. 56(d). But that rule only applies when facts are unavailable to a nonmovant, and here, Plaintiffs seek to file a supplemental motion for summary judgment, not a supplemental response to Guerra's motion for summary judgment. Reliance on Rule 56(d), moreover, is made when a party opposing summary judgment responds to such motion. And it requires a showing "by affidavit or declaration," which is lacking in this case as well.

have disobeyed the scheduling order or other pretrial order by filing their motion for leave. Untimeliness of a motion may be a reason to deny a requested supplementation, but it does not typically warrant sanctions absent specific disobedience of a pretrial order beyond the passing of a deadline.

## V. SUMMARY JUDGMENT STANDARD

"The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law."[7] Fed. R. Civ. P. 56(a). "As to materiality, the substantive law will identify which facts are material" and facts are "material" only if they "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Disputes over material facts qualify as "genuine" within the meaning of Rule 56 when "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* Given the required existence of a genuine dispute of material fact, "the mere existence of *some* alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment." *Id.* at 247-48. A claim lacks a genuine dispute for trial when "the record taken as a whole could not lead a rational trier of fact to find for the nonmoving party." *Scott v. Harris*, 550 U.S. 372, 380 (2007) (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986)).

The "party seeking summary judgment always bears the initial responsibility of informing the district court of the basis for its motion." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). This includes identifying those portions of the record that the party contends demonstrate the absence of a genuine dispute of material fact. *Id.* When seeking summary judgment on an affirmative defense, the movant "must establish beyond peradventure" each essential element of the defense.

[7] The summary judgment standard "remains unchanged" despite 2010 amendments to Fed. R. Civ. P. 56 that replaced "issue" with "dispute." Fed. R. Civ. P. 56 advisory committee notes (2010 amend.). Although the standard remains the same, the Court utilizes the amended terminology even when relying on caselaw that predates the amendments.

*Access Mediquip LLC v. UnitedHealthcare Ins. Co.*, 662 F.3d 376, 378 (5th Cir. 2011), *adhered to on reh'g en banc*, 698 F.3d 229 (5th Cir. 2012); *Fontenot v. Upjohn Co.*, 780 F.2d 1190, 1194 (5th Cir. 1986).

But when "the nonmovant bears the burden of proof at trial, the movant may merely point to an absence of evidence, thus shifting to the non-movant the burden of demonstrating by competent summary judgment proof that there is [a genuine dispute] of material fact warranting trial." *Lyons v. Katy Indep. Sch. Dist.*, 964 F.3d 298, 301-02 (5th Cir. 2020) (quoting *In re: La. Crawfish Producers*, 852 F.3d 456, 462 (5th Cir. 2017)). The movant need not "negate the elements of the nonmovant's case." *Austin v. Kroger Tex., LP*, 864 F.3d 326, 335 (5th Cir. 2017) (emphasis omitted) (parenthetically quoting *Little v. Liquid Air Corp.*, 37 F.3d 1069, 1076 n.16 (5th Cir. 1994) (en banc)). In these instances, however, the movant must "point[] out that there is no evidence to support a *specific element* of the nonmovant's claim"; rather than making "a conclusory assertion that the nonmovant has no evidence to support his *case*." *Id.* at 335 n.10.

In considering a motion for summary judgment, courts view all facts and reasonable inferences drawn from the record "in the light most favorable to the party opposing the motion." *Heinsohn v. Carabin & Shaw, P.C.*, 832 F.3d 224, 234 (5th Cir. 2016) (citation omitted). Once the movant has carried its summary judgment burden, the burden shifts to the non-movant to establish a genuine dispute of material fact. With this shifting burden, the nonmoving party "must do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita*, 475 U.S. at 586. "Unsubstantiated assertions, improbable inferences, and unsupported speculation are not sufficient to defeat a motion for summary judgment." *Heinsohn*, 832 F.3d at 234 (citation omitted). Additionally, the courts have "no duty to search the record for material fact issues." *RSR Corp. v. Int'l Ins. Co.*, 612 F.3d 851, 857 (5th Cir. 2010); *accord Hernandez v. Yellow Transp., Inc.*, 670 F.3d 644, 651 (5th Cir. 2012).

## VI. COLLATERAL ESTOPPEL

Based upon an asserted collateral estoppel bar, Guerra seeks dismissal of all claims asserted by Dr. Cantu. *See* ECF No. 109 at 18-20. While seeking dismissal of all claims based on collateral estoppel, she focuses on deposition testimony from Dr. Cantu regarding what caused him severe emotional distress. *See id*. He testified as to what caused his emotional distress:

> Q: . . . What conduct of Dr. Guerra caused you to suffer severe emotional distress?
>
> . . .
>
> A: The first thing was withholding visitation of my children starting in 2018. Then alleging that I physically abused my children in a report to CPS shortly after that. And then hiring Digital Forensics Corporation to monitor us and access our internet and video surveillance system in our home.

*See* Dep. Cantu (ECF No. 109-3) 91:6-19.

Guerra purports to premise this bar on the above testimony, as well as a Mediated Settlement Agreement ("MSA") (ECF No. 109-9) and a resulting Motion for Dismissal With Prejudice (ECF No. 109-12)[8] filed by Dr. Cantu in relation to an enforcement/modification/custody suit initiated in Bexar County in May 2018. *See* ECF No. 109 at 19-20. She also asserts that Bexar County entered an order to dismiss with prejudice on December 4, 2019. *Id*. at 19. Plaintiffs simply respond that there is no collateral estoppel applicable in this case. *See* ECF No. 112 at 16.

The Court agrees that collateral estoppel does not warrant dismissal of any claim. As pled, Plaintiffs' intentional infliction of emotional distress claim results from Defendants' cyberstalking and malicious prosecution. *See* ECF No. 6 ¶¶ 122-24. Thus, Guerra's focus on severe emotional distress from the custody dispute does not address the intentional infliction of emotional distress asserted in this case. In addition, Dr. Cantu testified immediately after the above testimony that the identified conduct was not "all of the conduct" that he alleges caused him "to suffer from

[8] Although Guerra's briefing erroneously identifies this as Exhibit 10, *see* ECF No. 109 at 19 n.53, Exhibit 12 is the correct exhibit.

emotional distress." ECF No. 109-3, 91:21-25. Further, although Guerra provides a motion for dismissal, she does not provide the actual dismissal order. Moreover, the motion for dismissal only seeks dismissal of "all claims that were asserted by Rodrigo David Cantu against Sandra Guerra in this matter," i.e., the state custody case. *See* ECF No. 109-12. Notably, in its opening paragraph, the MSA states: "The undersigned parties to this settlement agreement agree to compromise and settle the stated claims and controversies between them as described on the attachments." ECF No. 109-9 at 1. No one disagrees that both Dr. Cantu and Dr. Guerra signed the MSA. An attachment to the MSA states that the MSA does two things: (1) modifies certain identified child provisions from prior final orders and (2) states that an enforcement/suspension of commitment order would be dismissed with prejudice. *See id* at 5 (Ex. A to MSA).

For all of these reasons, the Court finds that Guerra has not carried her burden to show that a collateral-estoppel bar entitles her to summary judgment on any claim. Accordingly, the Court denies Guerra's motion to the extent she seeks summary judgment on the basis of this affirmative defense. It thus proceeds to consider whether either side is entitled to summary judgment on the affirmative claims put at issue by the instant motions for summary judgment.

## VII. CFAA CLAIMS

Plaintiffs assert eight claims under the CFAA: (1) unauthorized access to a protected computer in violation of 18 U.S.C. § 1030(a)(2)(C), (2) unauthorized damage to a protected computer in violation of § 1030(a)(5)(A), (3) unauthorized access to a protected computer recklessly causing damage in violation of § 1030(a)(5)(B), (4) unauthorized access to a protected computer recklessly causing damage and loss in violation of § 1030(a)(5)(C), (5) conspiracy to commit unauthorized access to a protected computer in violation of §§ 1030(a)(2)(C) and 1030(b), (6) conspiracy to commit unauthorized damage to a protected computer in violation of §§ 1030(a)(5)(A) and 1030(b), (7) conspiracy to commit reckless damage to a protected computer in violation of §§ 1030(a)(5)(B) and 1030(b), and (8) conspiracy to commit unauthorized access to a protected

computer causing damage and loss in violation of §§ 1030(a)(5)(C) and 1030(b). *See* FAC ¶¶ 54-92. Both Guerra and Plaintiffs seek summary judgment on these claims.

Stated generally, Guerra seeks dismissal of these claims because Plaintiffs have no evidence that she intentionally or knowingly hacked or surveilled them. ECF No. 109 at 2. She later argues that Plaintiffs lack any competent evidence that she intentionally or knowingly accessed their computers or intentionally caused any damage. *Id*. at 6. The crux of this argument is that "Plaintiffs cannot meet their summary judgment burden to prove that Dr. Guerra acted with the requisite intent or knowledge required to give rise to liability under the CFAA." *Id*. Guerra also seeks summary judgment on these claims because Plaintiffs have no competent evidence that they incurred damages exceeding $5,000 during any one-year period. *Id*. at 2, 13-16. Plaintiffs on the other hand argue that they are entitled to summary judgment on these claims. *See* ECF No. 110 at 11-14.

Section 1030 of Title 18 of the United States Code governs fraud and related activity in connection with computers. This section has undergone several amendments since its enactment in 1996. The current version became effective on October 20, 2020, and added text related to elections and computers that are part of a voting system. Except for that added text, which has no bearing on this case, the statute has been the same since September 26, 2008. The Court thus cites to the current version because all relevant provisions are applicable for all aspects of this case. Due to various other amendments, some caselaw has become outdated or suspect.

Section 1030(a) makes enumerated acts unlawful. A violation of § 1030(a)(2)(C) occurs when one "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer." A violation of § 1030(a)(5) occurs when one

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.

> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Section 1030(b) makes it unlawful to conspire or attempt to conspire to commit a § 1030(a) offense.

The CFAA defines a number of pertinent terms. *See* 18 U.S.C. § 1030(e). To constitute a "computer" under the CFAA requires a "high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." *Id*. § 1030(e)(1). As relevant to this case, a protected computer is one "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *Id*. § 1030(e)(2)(B). And for purposes of the CFAA, "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id*. § 1030(e)(6). "The phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." *Van Buren v. United States*, 141 S. Ct. 1648, 1655 (2021).

"Civil actions are authorized for some, but not all, violations of § 1030's substantive provisions." *Fiber Sys. Int'l, Inc. v. Roehrs*, 470 F.3d 1150, 1156 (5th Cir. 2006). Section 1030(g) provides:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation

> involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

The context of this case makes only subclause (I) at issue, and it requires "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." *Id.* § 1030(c)(4)(A)(i)(I). Under the CFAA,

> the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

*Id.* § 1030(e)(11). "The term 'loss' . . . relates to costs caused by harm to computer data, programs, systems, or information services." *Van Buren v. United States*, 141 S. Ct. 1648, 1659-60 (2021). Further, "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). These provisions – § 1030(e)(8) and (11) – "specify what a plaintiff in a civil suit can recover." *Van Buren*, 141 S. Ct. at 1659.

To succeed on a CFAA claim, Plaintiffs not only must establish "the elements of a particular substantive offense" and show that they suffered "'damage or loss' due to th[e] offense," but they also "must establish one of the five types of conduct specified under subsection (c)(4)(A)(i)." *Donahue v. Tokyo Electron Am., Inc.*, No. A-14-CA-563-SS, 2014 WL 12479285, at *10 (W.D. Tex. Sept. 2, 2014). Here, that additional conduct is § 1030(c)(4)(A)(i)(I)'s monetary loss requirement. Further, in general, the CFAA requires as an essential element that the defendant access "a computer 'without authorization or exceeds authorized access.'" *Land & Bay Gauging, LLC v. Shor*, 623 F. App'x 674, 683 (5th Cir. 2015) (per curiam) (quoting *Hunn v. Dan Wilson Homes, Inc.*, 789 F.3d 573, 583-84 (5th Cir. 2015)). And each of Plaintiffs' CFAA claims require such element. Each claim also requires intentional and/or knowing conduct by the defendants. Courts

refer to this latter requirement as a "statutorily required mens rea." *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007); *accord United States v. Thomas*, 877 F.3d 591, 597 (5th Cir. 2017).

When a statute applies in both a criminal and civil context, courts "must interpret the statute consistently, whether [they] encounter its application in a criminal or noncriminal context." *Leocal v. Ashcroft*, 543 U.S. 1, 12 n.8 (2004). Further, "the rule of lenity applies" in such circumstances. *See id*. "The rule of lenity provides that when a choice must be made between two readings of what conduct Congress has made a crime, it is appropriate, before choosing the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *United States v. Palazzo*, 558 F.3d 400, 403 n.2 (5th Cir. 2009) (citation and internal quotation marks omitted). Courts apply "the rule of lenity" when a "statute is ambiguous." *Cargill v. Garland*, 57 F.4th 447, 469 (5th Cir. 2023) (en banc).

**A. Guerra's Challenge to CFAA Claims**

Guerra primarily challenges Plaintiffs' CFAA claims on grounds that Plaintiffs have no evidence that (1) she acted with the requisite intent or knowledge required to sustain a CFAA claim or (2) they incurred the requisite amount of "damages" to support a civil claim. ECF No. 109 at 6, 13. These challenges attack the evidentiary support for whether (1) she intentionally accessed a computer or protected computer in violation of the CFAA, (2) she knowingly caused the transmission of anything that intentionally caused damage to a protected computer, and (3) Plaintiffs have incurred loss in an amount of $5,000 or more in any one year. *See id*. at 6-16. The focus of the first prong is on intentional access, whereas the second prong concerns both the knowing and damage components.

However, despite that primary focus, Guerra also asserts that Plaintiffs lack any evidence that (3) either defendant hacked or surveilled them; (4) she caused any damage to Plaintiffs' computers; (5) she conducted any video surveillance; (6) she listened to conversations through any link sent to MC; (7) she hacked MC's computer and breached her VPN, firewall, and router; or (9)

either defendant was involved in stealing personal information of Dr. Cantu and placing such information on the dark web. *Id*. at 2, 6-10. By pointing to a lack of evidence to support these aspects of Plaintiffs' CFAA claims, Guerra has carried her summary judgment burden. The burden thus shifts to Plaintiffs to present evidence to establish a genuine dispute of material fact.

In response, Plaintiffs contend that competent evidence shows that Guerra accessed their computers causing damage and loss. ECF No. 112 at 7. They argue that the record indicates that "Guerra acted with the requisite knowledge and intent to give rise to liability under the CFAA." *Id*. at 8. With respect to the monetary loss requirement, they also argue that "Guerra confuses CFAA damages with CFAA loss." *Id*. at 12. They contend that "[d]amages under the CFAA have nothing to do with monetary loss and are specifically defined in nonmonetary terms." *Id*. (citing 18 U.S.C. § 1030(e)(8)). They further submit that they have provided ample evidence to overcome the $5,000 threshold. *Id*. at 12-15.

Plaintiffs, of course, cannot carry their burden on mere contention or argument without supporting evidence. Parties do not carry their burden with unsubstantiated assertions, improbable inferences, or unsupported speculation. In response, Plaintiffs provide twenty exhibits (Exs. A through T), although they do not cite to each one. Other than Exhibits S and T, these duplicate exhibits that Plaintiffs initially provided in support of their own motion for summary judgment. Before the Court considers Guerra's challenges in more detail, it first summarizes the evidence presented by Plaintiffs.

**1. <u>Presented Evidence</u>**

Plaintiffs contend that "Defendants planned and executed a conspiracy to purposely deploy phishing links to gain access to [MC's] computers." ECF No. at 112 at 8-9. They similarly contend that "[o]n August 21, 2018, Dr. Guerra intentionally followed DFC's guidance and used fake emails to send phishing links to the Plaintiffs." *Id*. at 9. As support they cite to Exhibit B (the Phase I Report), Exhibit H (actually Ex. E, emails purportedly forwarded from Guerra to DFC), Exhibit

G (testimony from DFC's expert), and Exhibit O (purported instructions from DFC to Guerra as to how to deploy the links). *See id*. at 9 nn.30, 32 (providing parenthetical commentary as to why the exhibits support the contentions).[9] But Plaintiffs overstate their proof. The cited evidence supports finding that Defendants planned to send tracking links to MC and that someone indeed sent at least one such link to her. And as discussed in more detail later, the evidence also supports a reasonable inference that Guerra sent at least one link to MC. But whether such conduct constitutes a conspiracy, phishing, or access to any computer is beyond the facts of these cited exhibits.

The Phase I Report speaks for itself, and the Court previously reviewed it in the background section. Although Plaintiffs purport to provide Exhibit O for *in camera* review, to date, the Court has not received it despite two emails from court staff requesting all withheld exhibits. Nevertheless, for purposes of the motions pending before it, the Court accepts at face-value Plaintiffs' parenthetical regarding Exhibit O to the extent that they state that DFC provided instruction to Guerra as to how to deploy the tracking links. The Phase I Report itself also includes some instruction in that regard.

As for Exhibits E and G, the Court has greater difficulty in accepting them at face value. Although Plaintiffs parenthetically contend that Exhibit E are emails that Guerra forwarded to DFC from fake email addresses from which she had phished Plaintiffs by sending URL tracking links, they provide no evidence that Guerra indeed forwarded the emails. One can ascertain from Exhibit E that someone forwarded the emails to DFC. And one might suspect that it was Guerra, given her relationship with DFC and the results in the Phase I Report. But it would have been a simple matter for Plaintiffs to explain where they obtained the emails and why they affirmatively assert that Guerra forwarded the emails when the emails themselves do not show that. Instead of

[9] Because Plaintiffs later cite to this quartet of exhibits with the same parenthetical commentary, the Court will refer to the string citations as the quartet of exhibits when it later discusses them. Plaintiffs also rely on this quartet of exhibits in their motion for summary judgment. *See* ECF No. 110 at 11 n.33.

asserting that the Court can reasonably infer that Guerra forwarded the emails, Plaintiffs simply provide a parenthetical unsupported by the emails themselves. Nevertheless, for purposes of Guerra's summary judgment motion, the Court will reasonably infer that Guerra forwarded the emails to DFC and that Guerra and DFC sent tracking links to MC.

The parenthetical commentary as to testimony of DFC's expert is likewise questionable. First, the parentheticals often use the charged term, "phishing," when the expert specifically declined to accept that characterization of the tracking links. *See* Ex. G 24:5-8. And, while the expert testified that it is possible to introduce malware through a phishing link, *id*. 30:12-22, he further testified that the code contained in the tracking link lacked the capabilities for that type of attack, *id*. 31:13-25. It thus appears that Plaintiffs attempt to take unwarranted liberties with the expert's testimony. And, even though the Court makes all reasonable inferences in Plaintiffs' favor and views the evidence in the light most favorable to Plaintiffs when considering Guerra's motion, the Court does not view the expert's testimony as providing a reasonable inference that Plaintiffs suggest in some parentheticals. Relying on DFC's expert to support possibilities that the expert himself testified were not present from his review of the tracking links amounts to no more than unsupported speculation. Plaintiffs have provided no evidence from their own computer expert or from their own computer forensics investigator to counter testimony of DFC's expert.

Plaintiffs further contend that "[a]fter successfully deploying the phishing links against Plaintiffs, Dr. Guerra forwarded the phishing emails to DFC, in a display of purpose and intent." ECF No. at 112 at 9. As support she cites to Exhibit D with a parenthetical that the exhibit shows discussions of "URL tracking links deployed against Plaintiffs." *Id*. at 9 n.33. Like Exhibit O, Plaintiffs withheld Exhibit D subject to *in camera* review, but have not provided the exhibit to date. Perhaps this exhibit connects the dots missing in many of Plaintiffs' contentions. But even accepting the parenthetical commentary as accurate, such commentary is not enough to connect the missing dots. In any event, the Court has reasonably inferred that Guerra forwarded the emails

in Ex. E to DFC.

Plaintiffs next contend: "Once Dr. Guerra acquires access to Plaintiffs' computer network, she worked with DFC to infiltrate Plaintiffs' computer networks, impairing the integrity and availability of the data on that network in violation of 18 USC § 1030(a)(5)(A), 18 USC § 1030(a)(5)(B) and 18 USC § 1030(a)(5)(C)." *Id*. at 9. Plaintiffs then argue and contend:

> Once Plaintiffs' network was compromised, Dr. Guerra and DFC had free access to surveil the Plaintiffs. The connection established by DFC and Dr. Guerra damaged Plaintiffs' computer network. The threshold for damage under the CFAA is minimal and only requires any impairment to the integrity or availability of the data. Computer intrusions by their nature compromise the integrity of their data. A network disruption caused by surveillance software constitutes impairment to the availability of data. This necessitated Plaintiff's [sic] hiring of computer experts to deal with the network intrusion.

*Id*. 10-11. Plaintiffs do not cite any evidentiary support for any of these arguments and contentions, except for the last sentence. *See id*. at 10-11 & n.35. And for that last sentence, they cite to Exhibits P and Q, which provide receipts for various computer-related matters. While those receipts show that Plaintiffs hired a computer expert and paid for various computer-related matters, neither exhibit shows why Plaintiffs hired the expert or incurred the other costs.

Plaintiffs later contend that Guerra "incorrectly claims" that "Spectrum Cable installed the wire splicer found on Plaintiffs' internet cable running to their home" when "Spectrum actually determined that the cable splitter was not installed by them and removed it." *Id*. at 11. For the second quoted language, Plaintiffs cite to Exhibit F, *id*. at 11 n.36, which is service appointment scheduling and billing from Spectrum with photos of cable splicing. However, nothing within Exhibit F indicates that the cable company determined that it did not install the splicer. Nothing indicates that the company even removed the splicer. Nothing counters Guerra's evidence that the cable company reported to MC's employer that the splitter "appears to have been attached by Spectrum cable" for unknown reasons. *See* ECF No. 109-2 at 74.

Plaintiffs further contend that Dr. Cantu's personal information was compromised as

shown by the fact "that DFC had compiled a report on Dr. Cantu that included his personal information, including his . . . complete Social Security number, which was later found for sale on the dark web." ECF No. at 112 at 11-12. As support they cite to Exhibit N, another exhibit withheld subject to *in camera* review, and to Exhibit A, the retainer agreement between Guerra and DFC. *See id*. at 12 n.38. According to a parenthetical, Exhibit N provides communications between Guerra and DFC. *Id*. The retainer agreement (Ex. A) does not support finding that Dr. Cantu's personal information was compromised. Whether Exhibit N supports such a finding is uncertain. But from the evidentiary submissions before it, the Court cannot make any reasonable inference that Dr. Cantu's information was compromised merely because DFC compiled a report that included his complete social security number and that the number was later found for sale on the dark web.

Plaintiffs also contend that competent summary judgment evidence shows that Defendants caused more than the $5,000 loss required by the CFAA. *See id*. at 12-15. As support they attach billing records of a computer consultant (Ex. P), Spectrum Cable (Ex. F), and medical providers (Ex. S). *See id*. 12-15 nn. 41-51. To the extent necessary, the Court will address these exhibits more fully later.

When addressing their alleged HACA violation, Plaintiffs contend that "Guerra knowingly sent Plaintiffs phishing links"; "DFC guided Dr. Guerra on accessing Plaintiffs' networks"; and after "establish[ing] access, Dr. Guerra and DFC knowingly acted with intent to obtain information from, and damage, Plaintiffs' computer network." *Id*. at 15. They only provide cited evidentiary support for the second of the quoted language. *See id*. at 15 n.52. And that support consists of the quartet of exhibits discussed previously. Viewing the evidence in the light most favorable to Plaintiffs, the cited evidence supports finding that Guerra intentionally or knowingly sent tracking links and that DFC guided her in that endeavor. While Defendants intended to obtain tracking information, the evidence is insufficient to show any intent to damage any computer. And whether the

conduct may constitute accessing a computer is a matter addressed later.

When addressing their wiretap claim, Plaintiffs concede that they do not contend that Guerra installed the cable splitter. *Id*. at 15. They instead contend that, because Guerra hired DFC and DFC's expert "demonstrated a high level of knowledge of coaxial wiretapping," a "reasonable jury could find that Defendants violated Federal Wiretap law by splicing into Plaintiffs' network." *Id*. As support, they cite to Exhibit G, the deposition of DFC's expert, which shows that the expert had knowledge of splicing techniques and that he evaded answering some questions. *See id*. at 15 n.53. They also state without support that "Spectrum Cable visited Plaintiffs' home in-person and discovered that the cable splitter was not installed by anyone from their company." *Id*. at 16.

As noted previously when discussing Exhibit F, nothing within that exhibit indicates that the cable company determined that it did not install the splitter. And nothing counters Guerra's evidence that the cable company reported that the splitter "appears to have been attached by Spectrum cable" for unknown reasons. *See* ECF No. 109-2 at 74. Furthermore, the Court has previously discussed the expert's testimony in the background section. The cited deposition testimony does not support a reasonable inference that DFC's expert installed the cable splitter or spliced the cable. The expert testified that he had only installed such a device once and it was when he worked for an internet service provider. The Court will not indulge the speculation needed to infer that he was involved in any events leading up to this case. And as a forensics expert for DFC, it is unsurprising that he has knowledge of coaxial wiretapping.

With this evidence in mind, the Court proceeds to the specific matters challenged by Guerra in her motion for summary judgment. As an initial matter, this requires some review of the premise for Plaintiffs' CFAA claims.

**2. <u>Premise of CFAA Claims</u>**

Plaintiffs assert eight claims under the CFAA, predicating the first four on specific alleged conduct by Defendants and the last four on conspiring to commit such alleged conduct. As framed

in the First Amended Complaint, the alleged predicate acts concern a combination of alleged unauthorized access and unauthorized damage. Because there is no damage component to 18 U.S.C.§ 1030(a)(2)(C), Claim 1 only concerns unauthorized access. On the other hand, Claim 2 brought under § 1030(a)(5)(A) has no unauthorized access component and thus only concerns unauthorized damage. The two remaining non-conspiracy claims (Claims 3 and 4) have both components – unauthorized access and unauthorized damage. Claims 5 through 8 (the conspiracy claims) parallel Claims 1 through 4 while adding a conspiracy element.

The alleged "unauthorized access includes phishing Plaintiffs with fraudulent tracking URLs, wiretapping the Cantus' cable internet connection to their home and monitoring network traffic, and the use of surveillance malware against the Plaintiffs." FAC ¶¶ 57, 65, 70. The alleged computer

> damage includes impairment to the integrity and availability of the Cantus' data, programs, systems, and information on the Cantus' computers and networks resulting from computer crashes, diminished bandwidth, diminished processing time, and the deletion and alteration of data, all caused by Defendants' phishing, wiretapping, malware, and use of malicious codes against Plaintiffs.

*Id*. ¶¶ 61, 66, 71.

As reflected in the summary judgment briefing, Plaintiffs premise their computer fraud claims on two discrete acts – accessing their home computer through a splitter placed on a coaxial cable and accessing their computers through a link sent to MC's phone. ECF No. 110 at 11-14; ECF No. 112 at 8-12. The latter premise is that Guerra or DFC sent MC a link, which she clicked, thereby sending the device's IP address, geolocation, and operating system information to the sender. Plaintiffs characterize Defendants' plan as "to purposely deploy phishing links to gain access to Plaintiffs' computers." ECF No. 112 at 8-9; accord ECF No. 110 at 11 ("Defendants used phishing links to gain unauthorized access to . . . protected computers."). The unauthorized access occurred when the clicked link provided the means to transmit information to the link's sender.

Guerra has challenged the evidentiary support of Plaintiffs' unauthorized access and damage claims. By pointing to a lack of evidence, Guerra has carried her summary judgment burden and shifts the burden to Plaintiffs to provide evidentiary support.

As reflected in the discussion of submitted summary judgment evidence, Plaintiffs have failed to provide evidence to support their underlying premise in several respects. As for the alleged unauthorized access, Plaintiffs only provide evidence to support their claim that someone sent MC a tracking link that provided access to their computers. They provide evidence that DFC created tracking links and that MC received at least one link. Because Plaintiffs are resisting summary judgment at this point, the Court reasonably construes the facts as showing that Guerra sent at least one tracking link to MC.

But Plaintiffs provide no evidence that either defendant wiretapped their cable internet connection, monitored network traffic, or used surveillance malware against them. Nor have they provided any evidence to support finding that either defendant placed a cable splitter or spliced their cable. While they attribute these acts to Defendants, or more specifically, DFC through its computer expert, they completely fail to present evidence to support even a reasonable inference that DFC's expert was involved.

As for unauthorized damage, Plaintiffs provide no evidence of any of the alleged damage to their computers. An intrusion into a computer is insufficient of itself to show damage to the computer within the meaning of the CFAA. While not cited in response to Guerra's summary judgment motion, Plaintiffs do provide deposition testimony from Dr. Cantu that "DFC decreased the firewall in [MC's] private residence." Dep. Cantu 17:5-18:21 (Ex. R). But all he had as evidence of such decrease was Guerra's hiring of DFC and "their access of the internet." *Id*. 17:9-11. He testified that DFC "sent a link to [MC] that allowed them to access our system." *Id*. 17:18-19. He explained that MC's "portable cellular device was connected to our home internet system and, therefore, exposed our home internet system to what was on that link." *Id*. 17:25-18:3. As to what

evidence Dr. Cantu had that the "link caused the decrease in the firewall," he stated: "We didn't do it ourselves. No one else had access except for DFC through that link." *Id*. 18:6-7. He further testified that "DFC caused the firewall to be entirely turned off" and he based such testimony on the link that DFC sent to MC's phone – "that's the evidence [he has] that DFC accessed our internet." *Id*. 18:13-21.

Standing alone Dr. Cantu's deposition testimony is based entirely on speculation and conjecture. There is no evidence that the link sent to MC had the capability to turn off the firewall at her private residence. The fact that MC clicked on a link sent to her phone by DFC or Guerra provides no reasonable basis for concluding that the link turned off the firewall on her home computer system. Even had Plaintiffs cited to this deposition testimony, the testimony of Dr. Cantu provides insufficient support for finding that either defendant intended to damage or did damage any computer.

Nor have Plaintiffs presented evidence of any wiretapping or use of malware or malicious codes against them. As already discussed, Plaintiffs have presented no evidence that connects either defendant to placing the cable splitter or splicing cable. Therefore, any damage to a computer from the splitter placement or splicing cannot be attributed to either defendant.

Although Plaintiffs have shown that tracking links were sent to MC, they have presented no evidence to show that the code within such links was capable of damaging their computers or doing anything but sending certain identifying information to the sender when the recipient clicked the link. There is no evidence that any link damaged any computer or that anyone intended damage to a computer.

Thus, based on the summary judgment evidence provided by Plaintiffs, the only remaining premise for their CFAA claims is the tracking links sent to MC. And without evidence of damage to a computer, Plaintiffs' Claims 2, 3, 4, 6, 7, and 8 necessarily fail. However, a violation of 18

U.S.C. § 1030(a)(2)(C) and the related conspiracy claim have no requirement regarding damage to a computer. But that statute does include a mens rea requirement that the Court addresses next.

**3. Mens Rea Requirement**

As noted earlier, each of Plaintiffs' CFAA claims have a mens rea requirement. Violating 18 U.S.C. § 1030(a)(5)(A) through (C) requires knowing or intentional conduct that causes damage. As just discussed, Plaintiffs have presented no evidence of any damage to their computers that is attributed to MC clicking on a tracking link sent by either defendant. They have also not shown that either defendant intended to damage any computer. Thus, Plaintiffs' claims based on these provisions and their related conspiracy offenses fail to survive summary judgment.

Violating § 1030(a)(2)(C) and its related conspiracy offense require intentional access of a computer that obtains information from a protected computer but have no damage requirement. Given the above analysis, Plaintiffs' § 1030(a)(2)(C) claim now relates only to the tracking links sent to MC. And, based upon the Phase I Report, Guerra knew that the purpose of the DFC-created tracking URLs was to "capture[] IP address, operating system, browser, screen resolution, and hash information for the device from which the tracking URL is clicked." *See* Ex. 77. Even though the submitted Phase I Report did not come into existence until the day after links were sent to MC, the entirety of the circumstances provide a reasonable inference that Guerra knew when she sent the tracking links to MC that, if clicked, the links would transmit certain data back to her or DFC. The question is whether the evidence shows or is at least sufficient to support a reasonable inference that Guerra intentionally accessed a computer by sending a tracking link. However, for the reasons in the next section, the Court need not determine whether such knowledge equates to intentionally accessing a computer and thereby obtaining information from the computer in violation of § 1030(a)(2)(C).

**4. Monetary Loss Requirement**

The monetary loss requirement of 18 U.S.C. § 1030(c)(4)(A)(i)(I) has two components.

First, there must be a loss as defined by § 1030(e)(11). Second, the loss must aggregate at least $5,000 in value during any one-year period.

Section 1030(e)(11) broadly defines "loss" as "any reasonable cost to any victim" and then sets out representative examples in an "including" clause. In full that clause states: "including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." There has been some disagreement as to whether this clause requires that any loss be the result of an interruption in service. *See Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1173-74 (11th Cir. 2017) (discussing disagreement).

Although the Fifth Circuit has not weighed in on that issue, other circuits have concluded that:

> The plain language of the statutory definition includes two separate types of loss: (1) reasonable costs incurred in connection with such activities as responding to a violation, assessing the damage done, and restoring the affected data, program system, or information to its condition prior to the violation; and (2) any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

*See id.* at 1174 (agreeing with Fourth and Sixth Circuits). Because Congress wrote § 1030(e)(11) "in the disjunctive . . . the first type of loss [is] independent of an interruption of service." *Id.* Consequently, "'[l]oss' includes the direct costs of responding to the violation in the first portion of the definition, and consequential damages resulting from interruption of service in the second." *Id.* Further, because of the broad definition of "loss" in § 1030(e)(11), the Eleventh Circuit has rejected the contention that "there can be no loss under the CFAA unless it relates to fixing damage to a computer or network." *Id.* at 1175 n.2.

Until the Fifth Circuit or United States Supreme Court weighs in, this Court will utilize the Eleventh Circuit's persuasive interpretation of § 1030(e)(11). It will thus utilize this framework

when considering whether Plaintiffs have produced evidence to carry the burden that shifted to them when Guerra moved for summary judgment based upon a lack of evidence that Plaintiffs satisfy the monetary loss requirement.

Plaintiffs provide various billing records to show that they satisfy the $5,000 requirement. *See* Ex. P. The exhibit presents the following evidence.[10]

> 1. Monthly payments of $108.24 to CDR Business IT Solutions, LLC from MC commencing on January 1, 2020, and continuing through June 1, 2022.
>
> 2. A representative invoice showing that the $108.24 payment was a monthly router license fee and sales tax.
>
> 3. A January 15, 2019 invoice (# 111470) showing that MC returned a router for $649.99 credit and purchased an advanced security firewall router for $999.99 with an additional installation labor cost of $219.98.
>
> 4. A summary that shows Invoice # 111470 listed in accounts receivable along with a one-year license fee of $811.85 and other monthly charges of $108.24 for management and monitoring of secure router from January 2019 through January 2020. It also shows undeposited payments of various amounts for unspecified costs in 2019.
>
> 5. A $5,000 retainer fee paid on January 3, 2019, for a digital forensic investigation to be conducted by Computer Forensic Investigations, LLC ("EACFI").
>
> 6. A January 24, 2019 invoice for $274.89 for a dark web email live web scan.
>
> 7. Eight 2019 invoices for $108.24 each for monthly storage of data.
>
> 8. A February 23, 2019 invoice for $216.50 for an internal hard drive with case data.
>
> 9. A July 22, 2019 invoice for $237.38 for consultation services and travel expenses by EACFI.
>
> 10. An August 1, 2019 invoice for $1,034.24 to EACFI for two forensic analysis reports and a notary signature.
>
> 11. An EACFI summary of invoices for MC reiterating Items 5 through 10 and showing an unspecified $7,036.24 expense for January 7, 2019.

[10] Exhibit P is a twenty-eight-page document (not counting Exhibit P cover page) that unfortunately contains a few pages that simply duplicate information of other pages. Pages 14 and15 are exact duplicates and pages 20 through 27 duplicate information of earlier pages. When supporting a position, counsel should not provide duplicate information – at least without noting the duplication.

*See* Ex. P.

Notably, Plaintiffs present no evidence of any interruption of service. Their alleged loss, therefore, necessarily falls under the first type, i.e., direct costs incurred in responding to the violation. Although Plaintiffs present numerous receipts related to computer expenditures, they present nothing to show that they directly incurred these costs in responding to a CFAA violation by either defendant. Not only have they presented no evidence to connect the costs incurred to a CFAA violation, but they have also made no evidentiary showing that such costs were reasonable within the meaning of the statute.

On the facts presented, there is only one potentially viable CFAA violation in this case – one based on intentional access of Plaintiffs' computer through a clicked tracking link sent to MC thereby transmitting certain identifying information back to the sender. While Plaintiffs incurred a $5,000 retainer fee for CFI and obtained two forensic analysis reports for an apparent additional $1,034.24, Plaintiffs provide no report or other evidentiary support for connecting the costs incurred to responding to the tracking link, assessing what damage may have been done, or restoring any affected data, program system, or information to its condition prior to the violation. Indeed, the summary judgment evidence does not show that any damage resulted from MC clicking on any link provided by a defendant. Similarly, there is no summary judgment evidence that any restoration was required as a result of any such clicked link. From the summary judgment evidence provided, clicking on any tracking link from any defendant would merely result in certain identifying information being transmitted to the sender. During the relevant time-period, Plaintiffs had issues with a cable splitter and cable splicing that have not been attributed to either defendant. To be included in the $5,000 loss requirement, incurred costs must relate to a CFAA violation. Plaintiffs have not carried their burden to show that they satisfy the $5,000 loss requirement.

By failing to carry their summary judgment burden to present evidence of the $5,000 loss required to pursue a civil action under the CFAA, Plaintiffs doom all of their CFAA claims and

entitle Defendants to summary judgment on such claims. For these reasons, the Court grants Guerra's motion for summary judgment with respect to Plaintiffs' CFAA claims.

**B. Plaintiffs' Motion for Summary Judgment**

This failure also dispenses with any need to consider Plaintiffs' own motion for summary judgment as it relates to the CFAA claims. When a party fails to carry their burden as an opponent to summary judgment while enjoying the benefit of the favorable review of the evidence received as such an opponent, such a party cannot succeed on their own motion for summary judgment on the same evidence. Plaintiffs rely on the same evidence and make the same arguments in their own motion. *See* ECF No. 110 at 11-14. The arguments and evidence do not become more convincing when viewed in the light most favorable to the Defendants. The Court thus denies Plaintiffs' motion to the extent Plaintiffs seek summary judgment on their CFAA claims.

## VIII. HACA CLAIMS

Guerra argues that the same reasons asserted against Plaintiffs' CFAA claims entitles her to summary judgment on Plaintiffs' claims under the Harmful Access By Computers Act. ECF No. 109 at 15-17. By pointing to a lack of evidence to support the knowing and intent elements of the HACA claims, *id*. at 17, Guerra has carried her summary judgment burden and shifts the burden to Plaintiffs to support their claims with evidence.

When considering a claim based on state law, courts naturally apply state law to determine whether the claim survives a motion for summary judgment. *See Wilson v. Monarch Paper Co.*, 939 F.2d 1138, 1142 (5th Cir. 1991). Texas provides "a civil cause of action" for persons who are "injured or whose property has been injured as a result of a [knowing or intentional] violation of Chapter 33" of the Texas Penal Code. *See* Tex. Civ. Prac. & Rem. Code § 143.001(a).

Plaintiffs allege violations of Texas Penal Code §§ 33.02(a), 33.02(b-1)(1), and 33.022. *See* FAC ¶¶ 93-108. Section 33.02 governs breaches of computer security. A person violates § 33.02(a) when "the person knowingly accesses a computer, computer network, or computer system

without the effective consent of the owner." As held by a Texas court of appeals, "the knowledge requirement applies to both the access and the consent elements of the offense." *Muhammed v. State*, 331 S.W.3d 187, 192 (Tex. App. – Houston [14th Dist.] 2011, pet. ref'd). Despite two subsequent amendments of the statute as a whole, subsection (a) remains the same as it was when the court of appeals decided *Muhammed* in January 2011. If a person violates § 33.02(a), he or she also violates § 33.02(b-1)(1) if he or she had "the intent to defraud or harm another or alter, damage, or delete property."

Section 33.022 governs interference with electronic access. Except for network providers or online service providers "acting for a legitimate business purpose," a person violates § 33.022 when he or she "intentionally interrupts or suspends access to a computer system or computer network without the effective consent of the owner."

Like their CFAA claims, Plaintiffs premise their "knowing access" HACA claims on "Defendants phishing Plaintiffs with fraudulent tracking URLs, wiretapping Plaintiffs' home cable internet connection, monitoring their network traffic, and the use of surveillance malware and malicious codes against the Plaintiffs." FAC ¶¶ 95, 100. And like their CFAA claims, Plaintiffs provide no evidence supporting their alleged premise beyond the sending of tracking links.

Plaintiffs assert that, for the same reasons asserted for the CFAA claims, "the record establishes that Defendants acted with knowledge and intent and violated Texas's Harmful Access by a Computer Act." ECF No. 112 at 15. They rely on no additional summary judgment evidence. They have not carried their summary judgment burden as to claims predicated on violations of § 33.02(b-1)(1) or § 33.022, which include intent elements that are unsupported by the evidentiary record. Plaintiffs have provided no evidence that either defendant had any intent other than to send tracking links to MC in an effort to obtain identifying information.

Whether that intent is enough to satisfy § 33.02(a) requires closer examination. Violations of § 33.02(a) have three components: (1) knowing access; (2) of "a computer, computer network,

or computer system" (3) without effective consent. Texas has defined the latter two components, *see* § 33.01(4), (5), (8), (12); and they are not at issue beyond the knowledge component. Plaintiffs allege that Defendants accessed their computers through the tracking link sent to MC.

Texas defines "Access" as "to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system." Texas Penal Code § 33.01(1). Texas law also provides the following definition for "knowingly":

> A person acts knowingly, or with knowledge, with respect to the nature of his conduct or to circumstances surrounding his conduct when he is aware of the nature of his conduct or that the circumstances exist. A person acts knowingly, or with knowledge, with respect to a result of his conduct when he is aware that his conduct is reasonably certain to cause the result.

*Id*. § 6.03(b). This differs from the Texas definition regarding intent: "A person acts intentionally, or with intent, with respect to the nature of his conduct or to a result of his conduct when it is his conscious objective or desire to engage in the conduct or cause the result." *Id*. § 6.03(a).

Through § 33.02(a), Texas criminalizes a specific act as a breach of computer security – accessing a computer, computer network, or computer system – if done without effective consent. "Under Texas law, where specific acts are criminalized because of their very nature, a culpable mental state must apply to committing the act itself." *Moreno v. Dretke*, 450 F.3d 158, 172 (5th Cir. 2006) (citing *Cook v. State*, 884 S.W.2d 485, 487 (Tex. Crim. App. 1994)). Thus, one knowingly accesses a computer when one is aware that he or she is accessing a computer through his or her conduct. One does not knowingly access a computer without effective consent within the meaning of § 33.02(a) by merely sending an email or text. Such an act of itself does not breach any computer security. Nor does one knowingly access a computer without effective consent when a sent email or text contains a link intended to obtain access. While the intent of the link is to secure access without consent, such access does not occur until someone clicks the sent link.

Because § 33.02(a) criminalizes the act of access, it is insufficient to violate the statute by knowingly sending a link that may or may not gain access to a computer. The sender of such a link simply has no way to know whether he or she will actually access a computer without consent. The evidence in this case shows the creation of five different links and only one text or no more than a very limited number of texts or emails that were used to send the tracking link to MC. This case does not involve numerous recipients or numerous emails/texts that might change whether the sender knowingly accessed a computer by sending a link.

Section 33.02(a) does not criminalize acting knowingly with respect to a result of conduct, which is satisfied when one is aware that his or her conduct is reasonably certain to cause the result, i.e., access of a computer. But even if the statute focused on the result of the conduct, there is no evidence that either defendant in this case was aware that sending a link was reasonably certain to achieve access. Under the facts here, there is no reasonable certainty that MC, as the recipient of a sent tracking link, would click on the link thereby providing unauthorized access.

In short, one does not access a computer merely by sending a text or email (or a small number of texts or emails) with a link intended to gain access. In these circumstances, accessing the computer does not occur until the link is activated, which is beyond the knowledge of the sender. Plaintiffs have presented no evidence that Guerra was aware that she was accessing any computer when she sent a tracking link to MC. While there is evidence sufficient to reasonably infer that she intended to send the link so as to obtain certain identifying information, that intent differs materially from the knowing access required by § 33.02(a). That she may have intended to access Plaintiffs' computer through the included link does not suffice.

Because Plaintiffs have not carried their burden on their HACA claims, both defendants are entitled to summary judgment on such claims. Plaintiffs rely on the same arguments and evidence for their own motion for summary judgment. *See* ECF No. 110 at 14-15. The Court thus grants Guerra's motion for summary judgment and denies Plaintiffs' summary judgment motion

as they relate to the HACA claims.

## IX. WIRETAP CLAIM

Guerra argues that she is entitled to summary judgment on Plaintiffs' wiretap claim for similar reasons as to their CFAA and HACA claims. ECF No. 109 at 17-18. By pointing out that Plaintiffs lack evidence that she intentionally used any means to intercept communications of MC, *see id*., Guerra has carried her summary judgment burden.

Plaintiffs allege that defendants violated 18 U.S.C. § 2511 of the Federal Wiretap Act "by intentionally using, and endeavoring to use, any electronic, mechanical, or other device, including the installation of a cable line splitter and tracking URLs, to intercept Plaintiffs' wire, oral, or electronic communications." FAC ¶¶ 110-11. In general, § 2511 prohibits the interception and disclosure of wire, oral, or electronic communications. Plaintiffs rely on § 2511(1)(b), which provides for criminal penalties or governmental suit in certain circumstances for "any person who . . . intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication."

Section 2520 of Title 18 of the United States Code generally authorizes recovery of civil damages for "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." But Plaintiffs have presented no evidence that either defendant violated § 2511. There is simply no evidence of any device related to intercepting oral communication.

Because Plaintiffs have not carried their burden on their wiretap claim, both defendants are entitled to summary judgment on such claim. Plaintiffs do not move for summary judgment on this claim. *See* ECF No. 110 at 4 (omitting Claim 12 from list of claims at issue in Plaintiffs' motion for summary judgment). Nevertheless, Plaintiffs do contend that they are entitled to summary judgment on the wiretap claim. *See id*. at 8, 11. Not only is such contention insufficient to bring the matter before the Court, but Plaintiffs rely on the same evidence that failed to support

their CFAA claims. The evidence is likewise insufficient in the context of the wiretap claim. The Court thus grants Guerra's motion for summary judgment as it relates to the wiretap claim.

## X. MALICIOUS PROSECUTION

In addition to the claims already considered, Plaintiffs seek summary judgment on their state malicious prosecution claim. *See* ECF No. 110 at 8-10. Guerra urges the Court to deny this claim because Plaintiffs "cannot overcome the presumption of probable cause" and have "failed to conclusively establish as a matter of law that" (1) MC "was innocent of the charge" asserted against her; (2) "Defendants acted with malice"; and MC "suffered damages as a result of the criminal prosecution against her." ECF No. 114 1-2. DFC joins the opposition. *See* ECF No. 115 (Ex. B).

Texas law provides seven elements for a malicious prosecution claim. *Richey v. Brookshire Grocery Co.*, 952 S.W.2d 515, 517 (Tex. 1997). There must be "(1) the commencement of a criminal prosecution against the plaintiff;" (2) initiated or procured by the defendant in the civil case, which (3) terminated in favor of the plaintiff; (4) who was innocent of the charged offense. *Id*. In addition, there must be an (5) "absence of probable cause for the proceedings; (6) malice in filing the charge; and (7) damage to the plaintiff." *Id*. (altering paragraph structure).

Because Plaintiffs have not conclusively shown that MC was innocent of the charged offense of harassment, the Court denies summary judgment on this claim. In reply, Plaintiffs contend that "[t]he State dropped Dr. Guerra's malicious prosecution when it could not prove its case." ECF No. 118 at 3. Not only does it provide no evidence for that statement, but the record reflects that MC moved for dismissal of the charges on grounds of a speedy trial violation. *See* Ex. M. The fact that MC stated in the motion for dismissal that "the State could not prove its case, now, or ever," *see id.*, does not provide evidence of innocence. As this Court previously stated when ruling on a motion to dismiss, "public information shows that the charges were likely dismissed on grounds of speedy trial, which is not a reflection of the merits of the criminal action." *Cantu v.*

*Guerra*, No. SA-20-CV-0746-JKP-HJB, 2021 WL 2652933, at *9 (W.D. Tex. June 28, 2021). Given the evidentiary failing on this element of the malicious prosecution claim, the Court need not address the other elements. It denies Plaintiffs' motion for summary judgment as to this claim.

Because Plaintiffs have not carried their summary judgment burden on their own motion, the Court has no need to address arguments raised for the first time in a reply brief. And it is unnecessary to consider newly presented evidence with the reply. Nevertheless, in an abundance of caution, the Court has reviewed the new evidence submitted with the reply brief, i.e., Exhibits S and T that were also provided with Plaintiffs' response to Guerra's motion for summary judgment, as well as Exhibits U, V, and X, which are only included with the reply brief. Although the reply references an Exhibit W, *see* ECF No. 118 at 5 n.6, Plaintiffs have provided no such exhibit.

Exhibit U is largely unreadable given the magnification of the document, but the Court has no reason to doubt that it is a notice to Dr. Cantu regarding the suspension of his medical license, as indicated in the reply brief. *See* ECF No. 118 at 5 n.7. Exhibit V is an email dated September 11, 2011, where Guerra reminisces about her feelings regarding the tenth anniversary of the tragic events of September 11, 2001, and how shared her emotions with Dr. Cantu. Exhibit X provides additional detail about the agreement between MC and EACFI.

None of these exhibits alter the Court's view of the evidence or its rulings herein. While Exhibit X does provide some additional detail, it cannot satisfy Plaintiffs' burden that shifted to them when Guerra carried her summary judgment burden by pointing to a lack of evidence to support various aspects of Plaintiffs' claims. Plaintiffs simply did not proffer Exhibit X in response to Guerra's motion for summary judgment. Exhibit X, furthermore, does not cure the evidentiary deficiencies resulting in the granting of Guerra's motion for summary judgment. It does not show that investigation was limited to responding to the tracking link clicked on by MC in August 2018. It instead shows issues with a router in November 2018 and an investigation that went back to at least June 6, 2018. *See* Ex. X at 1719.

## XI. JUDGMENT INDEPENDENT OF MOTION

Rule 56(f) of the Federal Rules of Civil Procedure provides courts with discretionary authority to "grant summary judgment for a nonmovant" so long as they provide "notice and a reasonable time to respond." As stated in numerous instances throughout the Court's resolution of Guerra's motion for summary judgment, the failure of Plaintiffs to provide evidentiary support for required elements of their CFAA, HACA, and wiretap claims make summary judgment warranted for both defendants on those claims. The lack of evidence inures to the benefit of Defendant DFC even though it failed to move for summary judgment or join Guerra's motion. Thus, unless Plaintiffs provide a valid reason within fourteen days as to why the Court should not do so, the Court will grant summary judgment for DFC on the same basis that Guerra has obtained summary judgment on her motion. This fourteen-day period provides the notice and opportunity to be heard required by Fed. R. Civ. P. 56(f).

## XII. CONCLUSION

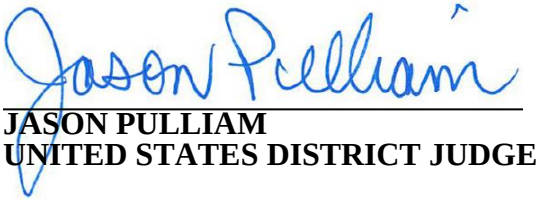
For the foregoing reasons, the Court **GRANTS IN PART AND DENIES IN PART** the *Motion for Summary Judgment* (ECF No. 109) filed by Defendant/Counter-plaintiff Dr. Sandra Guerra; **DENIES** the *Motion for Summary Judgment* (ECF No. 110) filed by Plaintiffs/Counter-defendants Melody Joy Cantu and Dr. Rodrigo Cantu; **DENIES** the *Motion for Leave to File Sur-Reply* (ECF No. 119) filed by Dr. Guerra; **DENIES** *Plaintiffs' Motion for Leave to File Supplemental Motion for Summary Judgment* (ECF No. 120); and **DENIES** the *Motion for Leave to File Defendants' Sur-Reply* (ECF No. 124) filed by Defendants related to the motion for leave to file supplemental motion.

The Court hereby dismisses Claims 1 through 12 asserted against Defendant Guerra. In accordance with Fed. R. Civ. P. 56(f), the Court has provided Plaintiffs notice and an opportunity to be heard as to why the Court should not dismiss those same claims as asserted against Defendant DFC. Regardless of any Rule 56(f) order of summary judgment, Plaintiffs may still pursue their

Claims 13 and 14 against both Defendants. And Guerra may still pursue her counterclaims except for the abuse-of-process claim that the Court dismissed earlier in this case.

**IT is so ORDERED.**

**SIGNED this 11th day of August 2023.**



**JASON PULLIAM**
**UNITED STATES DISTRICT JUDGE**